December 2004

The Role of Exercises in Training the Nation's Cyber First-Responders

Gregory White
University of Texas at San Antonio

Tim Goles
The University of Texas at San Antonio

The Role of Exercises in Training the Nation's Cyber First-Responders

Gregory B. White
Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
gwhite@utsa.edu

Timothy Goles
Department of Information Systems
The University of Texas at San Antonio
tgoles@utsa.edu

ABSTRACT

Terrorism has become a topic of much concern in this country since the events of September 11, 2001. As a result, an increased emphasis has been placed on training the nation's first-responders who will be called upon in the event of an attack to effectively respond to whatever the incident entails. Of growing interest is the possible use of cyber attacks as either the primary or a contributing mode of attack. As such, the need for a trained corps of cyber first-responders is increasing. Who are the nation's cyber first-responders and how best can they be trained to detect and respond to cyber attacks? One method that has seen some success is the use of scenario-based exercises to provide awareness and training to community cyber first-responders. A three-phased approach for such an exercise is proposed and initial results discussed.

Keywords

Computer Security, Information Security, Information Assurance, Scenarios, Training and Awareness.

INTRODUCTION

Much has changed in the United States since the events of September 11, 2001. Since then, the nation has become more interested in terrorism and security than ever in its history. Significant changes have occurred in the federal government and new legislation has passed with far-reaching impacts in the lives of the nation's citizens. The role of the first-responder during emergencies has been reviewed and discussed and their importance to their communities has resulted in increased federal funding for training and equipment. Normally when the term first-responder is mentioned people will think of fire and police departments but there is another type that has not received the attention that these others have. This additional category of emergency personnel are the cyber first-responders who must respond to cyber security events when they occur. While cyber events are often not dramatic and may not involve potential loss of life, there are times that events occur which could have a dramatic effect on the nation's economy and it's ability to function. While the nation is now seeing an increased emphasis placed on the training of fire and police first-responders, what is being done to educate those that will be a community's cyber first-responders? One approach is to conduct community and sector-based cyber exercises to promote awareness and to encourage information sharing and coordinated cyber responses at the community and sector levels.

WHAT IS A CYBER FIRST-RESPONDER

In many respects, every organization and every individual connected to the Internet is at some level a cyber first-responder. Every machine connected to the Internet has the possibility of being subverted and used in an attack on other systems – systems that might be involved in the control of one of the nation's critical infrastructures.

Most organizations are use to one of two types of cyber security events. The first are events that only appear to affect the organization itself. This includes unauthorized access to the organization's computer systems or a logic bomb set by a disgruntled employee. In both cases any damage is limited to the targeted organization and with the exception of possible regulatory issues that might force more public release or reporting of this information, the organization's natural tendency is to keep word of the incident quiet. The usual fear is that release of this sort of information will not do anything except provide bad publicity for the organization and bring unwanted media coverage or affect stock prices.

The second type of incident usually faced by organizations is one in which the general public is aware of the event as it is affecting many different organizations around the world. An example would be a virus or worm that indiscriminately attacks sites across the Internet. Events of this nature will frequently receive national media coverage and organizations, and individuals, can turn to their televisions to learn how they should respond. Additionally, there are a number of security

organizations, such as the US-CERT or the Department of Energy's CIAC that will post warnings about new cyber threats and the steps on how to protect against them.

Training for cyber first-responders is highly dependent on the organization the individual belongs to. Some employers may be able to afford dedicated security personnel who have the opportunity to stay current on newly discovered vulnerabilities. Others may rely on network administrators to fill the role of security administrator. Individuals may receive little training and have little time to dedicate to the security portion of their job. Individual home users, whose high-speed Internet access may also be exploited, are generally going to be even worse off and may have no training in, or awareness of, vulnerabilities that exist in their systems. All of these individuals, however, are part of the nation's cyber first-responders.

SCENARIO-BASED EXERCISES

There are three different reasons to conduct an exercise. The specific purpose will dictate the format for the exercise and how it will be conducted. The simplest is an awareness exercise whose purpose is to expose the participants to the threats and issues involved in the particular domain and make them aware of what their responsibilities are. The second is a training exercise in which the participants are cognizant of the security issues but are not trained in the most current technology or methods to address the domain threats. The last exercise is conducted in order to provide an opportunity for participants to be drilled in the processes, procedures, and use of the tools they have at their disposal in order to respond to events in the specific domain.

Exercises can be "live" in the sense that actual equipment or tools are used, such as when a fire department actually extinguishes a fire at a training facility or a network security administrator has to deal with electronic attacks on the network that have been launched by a penetration or "red" team. Live exercises are often expensive and can be hard to control when large numbers of individuals are involved. An alternative is to conduct a "tabletop" exercise in which a scenario has been created and events are discussed instead of simulated.

While there are obvious advantages to conducting live exercises , scenario-based tabletop exercises provide valuable training and can help organizations deal with uncertainty, since new or unique situations that may be hard to simulate can be addressed easily in this format.

Various agencies, such as the Department of Defense and the Nuclear Regulatory Commission, conduct "force-on-force" exercises designed to test the defenses of installations. Such exercises have been conducted for years and have focused on physical security. Recent extensions to such exercises have introduced cyber security and in some cases have actually featured it as the major focus of the exercise. The DoD has conducted this type of exercise since 1997 and refers to them as "No-notice Interoperability Exercises" (NIEX). A NIEX is designed to focus on command, control, communications, computers and intelligence interoperability issues. They are executed with little or no planning or notice to the participants. NIEX and Force-on-Force exercises represent the pinnacle of exercises utilizing the actual tools and methods that defenders would use in a real situation.

CYBER SECURITY EXERCISE EXAMPLES

In 1997, the DoD conducted its first large-scale exercise aimed at testing its ability to respond to attacks on the DoD information infrastructure. This exercise, known as Eligible Receiver, revealed a number of vulnerabilities in DoD information systems and the ability for personnel to respond to cyber attacks. The exercise included an actual attack on DoD information systems utilizing known vulnerabilities and open source tools. The exercise also included social engineering attacks in an attempt to gauge how familiar DoD personnel were to this form of attack and how well they had been trained to avoid falling prey to it.

In March 2002, the Air Force conducted what it referred to as an information warfare tactics development exercise which it called Black Demon. The exercise was designed to test the Air Force's approach to computer network defense and to evaluate how effective the approach was in addressing large-scale network attacks. Air Force bases around the nation were involved in this exercise that pitted network operators against opposing aggressor forces. The exercise was scenario-based and resulted in a number of recommendations to modify or add new tactics to the Air Force's procedures.

Both the DoD and Air Force exercises were "hands-on" exercises where participants had to deal with actual attacks conducted by an opposing force. In a tabletop exercise, events are presented in a paper scenario format with participants

sitting around a table discussing how they would respond. An exercise of this nature was the method used in the Pacific Northwest for the Blue Cascades exercise conducted in June 2002. Another difference between this and the other exercises discussed was that Blue Cascades' participants included individuals from both the public and private sectors. The exercise was designed to examine the participant's dependency upon various critical infrastructures and observe how an attack on one could have a cascading effect on others. Though not strictly a cyber event, the event has many parallels with a series of exercises being conducted for the various critical infrastructure sectors in cities around the nation.

Four of these sector-based tabletop exercises sponsored by the Information Sharing and Analysis Centers (ISACs) and the United States Secret Service (USSS) and conducted by the Center for Infrastructure Assurance and Security (CIAS) at the University of Texas at San Antonio (UTSA), have been completed. The first was held in New York for the financial services sector in March 2003. It focused on cyber related attacks on the financial services sector. This was followed by a second financial services tabletop exercise in Chicago in August 2003. Again the focus was on potential cyber attacks on the infrastructure. In November 2003 a third sector-based exercise was conducted, this time for the IT and Telecommunications sector near Silicon Valley in California. The fourth exercise of this type was held in February 2004 in Houston, Texas for the Oil and Gas Industry. This exercise deviated slightly from the previous three by introducing more physical attacks in conjunction with the electronic attacks that were presented but still remained with the tabletop format that had proven successful in serving as a training and awareness forum.

EXERCISES AS A TRAINING TOOL

Exercises of the type the DoD and Air Force conducted are dramatic, but only useful if the participants already have a good understanding of security and the procedures they are to follow and tools they are to use. For most communities this level of preparedness does not exist. In addition, though the DoD and Air Force are large, they each are still only a single organization. A community response will encompass many organizations and one of the most critical elements in a response is the communication that must take place between disparate organizations. From a cyber response perspective, very few cities have an understanding of the necessary lines of communication or even whom they should be communicating with. Until communities have a better understanding of what needs to be accomplished and how and who to communicate with, the more technical force-on-force exercises are a waste of time. Instead, what is needed are tabletop exercises designed to first make participants aware of the issues and second to help educate and train them on the procedures, tools, and communication channels required to address cyber attacks.

A three-phased approach was taken to accomplish this task for the Dark Screen exercise. Dark Screen was conducted between September 2002 and September 2003 in San Antonio, Texas by a team of community representatives from government, academia, and industry. The first phase consisted of a tabletop awareness exercise. Representatives from industry, local, state, and federal government, local critical infrastructures, and academia participated in a scenario-driven exercise that examined the ability for the city and surrounding community to detect and respond to a cyber attack.

The event explored the city's ability to recognize possible early indications or warnings of a pending attack and the ability to obtain this information from state or federal agencies. Later scenario events were designed to examine the ability of the various participants to work together to address an attack that is occurring. Responses to the various events by the participants were recorded and compiled for use in the second phase of the exercise.

The second phase commenced immediately after the conclusion of the tabletop exercise. During this phase participants took the lessons that were learned during the tabletop exercise and used them to enhance their organization's security posture. During this phase organizations also conducted vulnerability assessments and penetration tests which allowed for a more in-depth technical appraisal of their ability to respond to electronic attacks.

The final phase of the exercise provided an opportunity for participants to again come together to explore the community's ability to respond to a cyber security event. During a two-week period, various events were either simulated or in some limited cases were actually conducted to explore the detection and response capabilities for the various participants as well as to exercise the communication channels between organizations. In the event of a cyber attack on a city, the various entities within the city, including both government and industry organizations, need to cooperatively work together to coordinate the response.

Each of the three phases accomplished a different purpose with the overall goal being to enhance the community's ability to prevent, detect, and respond to a cyber security event. The first phase served to make all participants aware of the different

types of attacks that can occur, how the attacks can affect the various infrastructures, how the loss of one infrastructure can affect others, and prepare the communication channels between organizations that are needed to facilitate a timely and effective response to an attack. The second phase of the exercise provides an opportunity for individual organizations to train their cyber first-responders and to develop a security posture consisting of policies, procedures, personnel, and technology that will allow them to effectively respond. The final phase serves as an opportunity to exercise the communication channels that have been created and to test as a whole the community's ability to detect and respond to an electronic cyber attack.

The scenarios used in the first and third phases were of a different nature than what many cyber security personnel were familiar with. The events at first may have appeared to follow one of the two types of incidents described earlier – they appeared to either be a general attack with no real focus or appeared to be targeted solely at a single organization. In reality, what the scenarios depicted was an organized attack upon the city of San Antonio and various entities: public, private, and governmental. The premise or storyline involved a terrorist organization that was targeting the city as a result of specific events the city was involved in. The idea was to "discourage" the city and its citizens from supporting such activities by making a very public statement and disrupting their lives. Websites were defaced, various government agencies and local utilities attacked to disrupt services, and industry sectors, such as banking and financial institutions, were targeted to additionally cause confusion and concern among the citizens. Early probes were launched on various entities which, if they communicated information about these early attempts, might provide a picture of an unusual level of interest in the community that might allow officials and security experts to prepare for the more concerted attack that was to occur.

RESULTS

The three-phased approach to conducting a cyber exercise proved to be an effective format to train local San Antonio cyber first-responders in response procedures. Over 220 individuals participated during the first phase of the exercise conducted in San Antonio. The largest number came from the City of San Antonio, predominantly from their IT and emergency management offices. None of the individuals had ever participated in a cyber security exercise though many of the emergency services personnel had participated in other types of exercises. After the event, all of the participants reported a greater awareness of the potential for cyber attacks and the damage they could cause and went away with a resolve to better prepare for such an event. The single most frequently discussed lesson was the need for better communication during an event and the establishment of standardized procedures to provide to employees for them to follow in the event that a cyber attack occurred.

The second phase of the exercise provided the organizations the opportunity to develop or modify existing procedures in order to prepare for the final phase in which live attacks would be conducted. During this phase several organizations also conducted vulnerability assessments and penetration tests of their networks. For some this was the first time that they had an external organization conduct such a test and even though they had felt they were fairly secure, specific vulnerabilities were identified that could have allowed an attacker to disrupt services or take control of the organization's network. Problems consisted of both technical and procedural discrepancies and included a lack of any process for notifying other organizations when an incident occurred as well as common technical misconfigurations which could allow attackers to gain unauthorized access to systems. Using the results of the assessments performed, the organizations were able to enhance the security processes, procedures, and technology they used to protect their networks in advance of the third phase of the exercise.

In the third phase various organizations were probed and scanned electronically and more serious incidents simulated to test both the detection and response capabilities of the participating organizations. It was in this phase that the exercise could focus on the cyber first-responders as well as management personnel responsible for creation and enforcement of general security practices and procedures. While not extending to home users at this point, further exploration of how this can be accomplished needs to be conducted, the exercise still provided an opportunity for individuals tasked with protecting computer systems and networks to work with others as they collectively addressed an attack on the community in general.

How well the lessons learned on developing an exercise can be transported to other communities is still a question. There are many differences between the way communities are organized and run and a template general enough in nature to be applicable to a broad range of communities needs to be developed. Preliminary efforts to apply lessons learned in San Antonio to other communities have met with success. In February 2004, the same team from the CIAS conducted the first phase of a similar community exercise for Corpus Christi, Texas. Feedback from this event was as positive as the comments received after the San Antonio exercises. Participation yielded similar results to the San Antonio event with participant's knowledge of possible cyber attacks increased and the need for greater communication within the community recognized.

Plans are underway to continue with the second and third phase for Corpus Christi and data is being gathered to develop a template that may be transportable to other communities as well.

Another result of the San Antonio exercise has been the creation of an information sharing initiative in the community. The need for better communication between entities, especially during the early stages of a possible attack where indications and warnings might exist that could aid in the prevention of an attack, was recognized and a working group formed. This group, consisting of representatives from government, academia, and industry, is exploring better methods to share often sensitive information on incidents and events that others could benefit from as well. The group is looking to model the basic information sharing initiative after the successful Emergency Response Network in Dallas, Texas but is expanding upon this effort by examining ways to share more diverse information between industry sectors and government agencies.

CONCLUSION

Training cyber first-responders is no less important than training other first-responders. A general awareness of the possible threats and types of electronic attacks that can be launched against a community is important and is the first step in preparing communities for cyber attack responses. Teaching organizations who they should and must communicate with in the event of an attack is imperative to an effective response. Scenario-based cyber security exercises are proving to be an effective means of providing training and awareness to communities and individual critical infrastructure sectors. It is important that these events continue and, in fact, the efforts to conduct these should be expanded to every community in the nation to be conducted along with other disaster exercise drills they are use to performing. By doing so, the nation will be much better prepared to deal with an electronic attack, no matter what the source, when one occurs. Further study should be accomplished to examine how to extend the lessons learned during these exercises to other users in the community in order to expand the number of trained cyber first-responders.

REFERENCES

1. Cardonita, D (2002) Black Demon Tests Tactics Improves Network Defense, *Spokesman*, Summer 2002.
2. PNWER (2002) Initial Summary of BLUE CASCADES Infrastructure Interdependencies Exercise, June 2002, originally obtained from http://www.pnwer.org/pris/CascadesReport.htm.
3. Schoemaker, P. (1995), Scenario Planning: A Tool for Strategic Thinking, *Sloan Management Review*, (36:2), 1995, 25-40.
4. U.S. Nuclear Regulatory Commission (2004), Frequently Asked Questions about Force-on-Force Security Exercises at Nuclear Power Plants, February 2004, http://www.nrc.gov/what-we-do/safeguards/faq-force-on-force.html
5. White, G and Sanchez, J (2003) Dark Screen Sheds Light on Cyberspace Security Issues, *SIGNAL: AFCEA's International Journal*, Vol 57, No. 5, January 2003.